

Reversible data hiding with selective bits difference expansion and modulus function

Aulia Arham^{1,2}, Hanung Adi Nugroho², Domi Sepri¹

¹Department of Information Systems, Faculty of Science and Technology, Universitas Islam Negeri Imam Bonjol, Padang, Indonesia

²Department of Electrical and Information Engineering, Faculty of Engineering, Universitas Gadjah Mada, Yogyakarta, Indonesia

Article Info

Article history:

Received Apr 26, 2024

Revised Jan 24, 2025

Accepted Mar 11, 2025

Keywords:

Cryptography

Difference expansion

Information security

Reversible data hiding

Steganography

ABSTRACT

The integration of the internet of things (IoT) has significantly enhanced human life but also raises concerns about information security and privacy. Information security can be achieved through cryptography, which encrypts data to make it unreadable, or steganography, which hides data within other media. For sensitive media, such as military, medical, and forensic imaging, specialized techniques like reversible data hiding (RDH) are necessary to ensure the media can be fully restored after data extraction. Many researchers have proposed improvements to the RDH method in recent years. In this study, we propose an improved RDH method utilizing difference expansion and a modulus function. The method embeds data into the 4-bit, 3-bit, and 2-bit least significant bits (LSB) of the difference value of pixels, with a range of -2 and 2. The experimental findings demonstrate that our approach achieves an embedding capacity of 0.2507 bpp with 55.445 dB of peak signal-to-noise ratio (PSNR) for common images and 0.3849 bpp with 54.6810 dB of PSNR for medical images, using 2-bit difference values. The results demonstrate that our approach surpasses previous methods and holds promise for practical applications in IoT systems and the medical field, where secure and reversible data embedding is essential.

This is an open access article under the [CC BY-SA](#) license.



Corresponding Author:

Aulia Arham

Department of Information Systems, Faculty of Science and Technology

Universitas Islam Negeri Imam Bonjol

Sungai Bangek, Balai Gadang, Koto Tangah, Padang, West Sumatra, Indonesia

Email: auliaarham@uinib.ac.id

1. INTRODUCTION

In recent years, the internet of things (IoT) has transformed the manner in which devices communicate and interact, providing unmatched connectivity and convenience [1]. However, this interconnectivity raises significant concerns about data security and privacy. As IoT devices accumulate and swap extensive quantities of sensitive information, ensuring security information measures becomes essential. Security systems, notably cryptography and steganography, play pivotal roles in safeguarding IoT networks and data integrity [2]–[4]. Cryptography involves encoding data to secure its transmission and storage, making it incomprehensible to unauthorized parties [5], [6]. This technology, through encryption techniques, ensures data confidentiality, authentication, and integrity, reducing the likelihood of data breaches or unauthorized access in IoT ecosystems. Similarly, steganography, an art of concealing information within digital content [7], contributes to IoT security by embedding data in a manner that's imperceptible to the human eye or normal data transmission processes. This technique provides an added layer of security by hiding critical information within innocuous-looking data, preventing potential attackers from even recognizing the presence of concealed data.

In data hiding, three fundamental components form the core infrastructure: the sender, communication channel, and recipient [8], [9]. The sender is responsible for conveying sensitive data, while the recipient represents the intended party to receive this data. Facilitating the transfer process, the communication channel serves as the conduit for transmitting the data securely. Within the domain of digital image steganography, the process involves concealing confidential data within a chosen cover image. This concealment is carried out with precision, ensuring that the resulting stego image can be securely transmitted over unsecured public networks. The stego image, while appearing ordinary to casual observers, harbors concealed information, making it a covert carrier for the confidential data during transmission across potentially insecure channels. In other cases, the reversible data hiding (RDH) method is needed, such as in medical image, military, and forensic image applications where every bit of pixel is important information [10]–[14], Figure 1 illustrates the concept of RDH. After extracting the secret data, the RDH method can revert the image to its original state. This method is applied by expanding pixel value, which can be classified into three categories: difference: differential extension (DE), prediction-error expansion (PEE), and histogram shifting (HS).

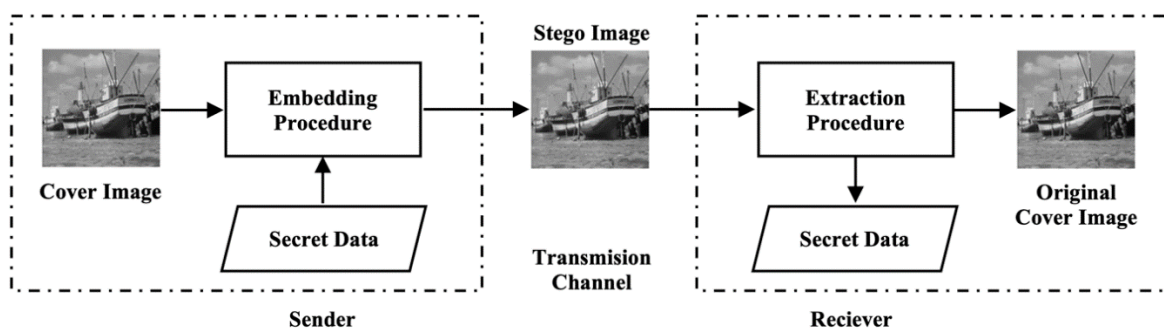


Figure 1. The concept of RDH methods

The initial introduction of the DE method can be traced back to the research conducted by [15]. This particular method showcases a highly promising reversible data embedding (RDE) technique with a substantial capacity. The cover image undergoes an integer wavelet transform, resulting in the acquisition of the difference values. These values are then expanded to create a space for RDH. Numerous subsequent studies have made significant improvements to this method [3], [16], [17]. In contrast to DE, which solely takes into consideration the correlation between two adjacent pixels, the PEE method exploits the local correlation within a larger neighborhood, thus yielding enhanced performance. PEE has garnered substantial attention due to its ability to harness the spatial redundancy present in natural images. Rather than regarding the difference operator as a decorrelation operation, PEE employs a pixel predictor. The initial proposal of PEE was put forth by Thodi and Rodriguez in [18], and since then, it has been widely adopted by numerous subsequent RDH works [19]–[23]. Alongside DE, HS stands as another highly successful approach for RDH. This approach involves the generation of a histogram, which is subsequently modified to achieve RDE. The first mention of HS-based RDH can be attributed to the work conducted by Ni *et al.* [24]. Moreover, the same concept surrounding HS was independently presented in recent years by [25]–[29].

This study intends to propose an improvement on the DE method previously introduced by Maniriho and Ahmad [3], based on a modulus function that can enhance capacity of embedding and visual quality. In this method, data embedding is carried out using the difference value of pixel pairs in the cover image. Data embedding is exclusively performed on difference values ranging from -2 to 2. To obtain the stego image, the pixel value of the cover image is concatenated with the difference value that has been embedded with data. The modulus function is used for extraction data and restoration of the cover image. Hossen *et al.* [17] suggested improving the method [3] by increasing the block size to 3×1 . The experimental results of this method demonstrate a significant increase in embedding capacity and visual quality.

The rest of this paper is organized as follows. Section 2 explains our approach in detail, covering the embedding and extraction processes, along with the computational complexities involved. Section 3 discusses the experimental results and offers a comparative analysis with earlier methods, focusing on aspects such as embedding capacity, performance, and visual quality. Finally, section 4 concludes the study by summarizing the main findings and presenting valuable insights derived from the data and research results.

2. METHOD

Improving the performance of data hiding methods is crucial for today's information security. To address this need, we propose a novel method to enhance the capabilities of existing techniques, especially those presented by previous researchers [3]. Our proposed method utilizes the difference values of 4-bit, 3-bit, and 2-bit LSB of pixels. This approach differs from the previous method [3], which employs 8-bit difference values from pixels. The consideration of using the LSB difference value of pixels can enhance embedding capacity, performance, and visual quality by reducing the range of difference values for pixel pairs. Data is embedded in a difference value between -2 to 2, similar to the previous method [3]. Figures 2 and 3 depict the processes of embedding and extracting in our method.

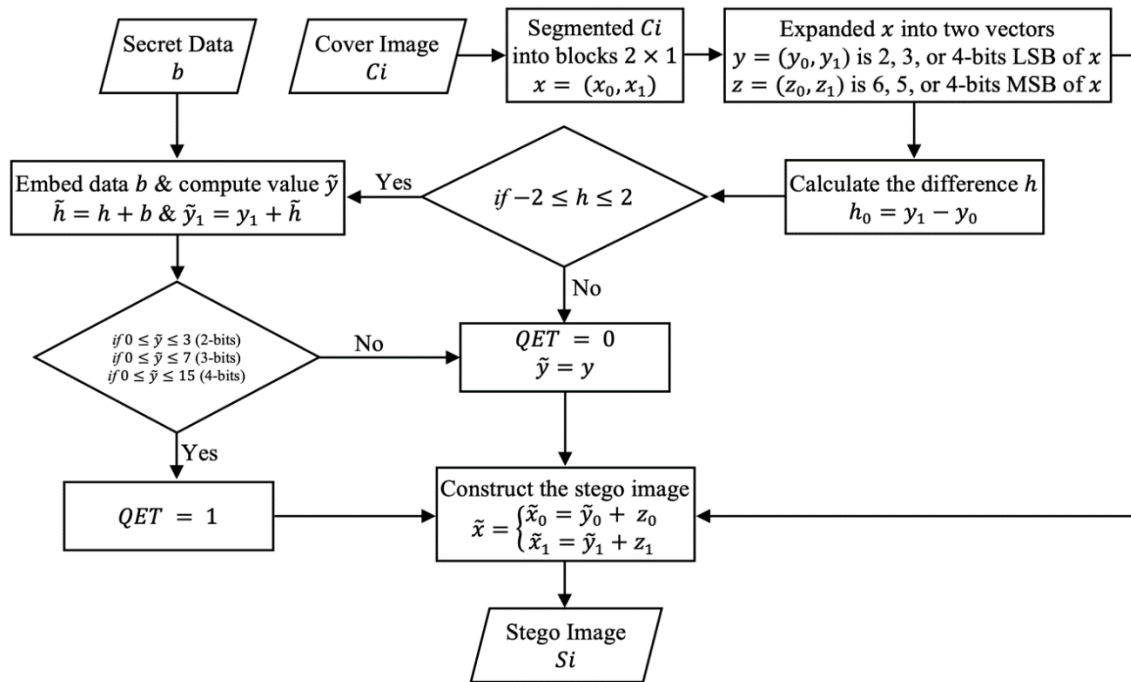


Figure 2. Embedding process for our method

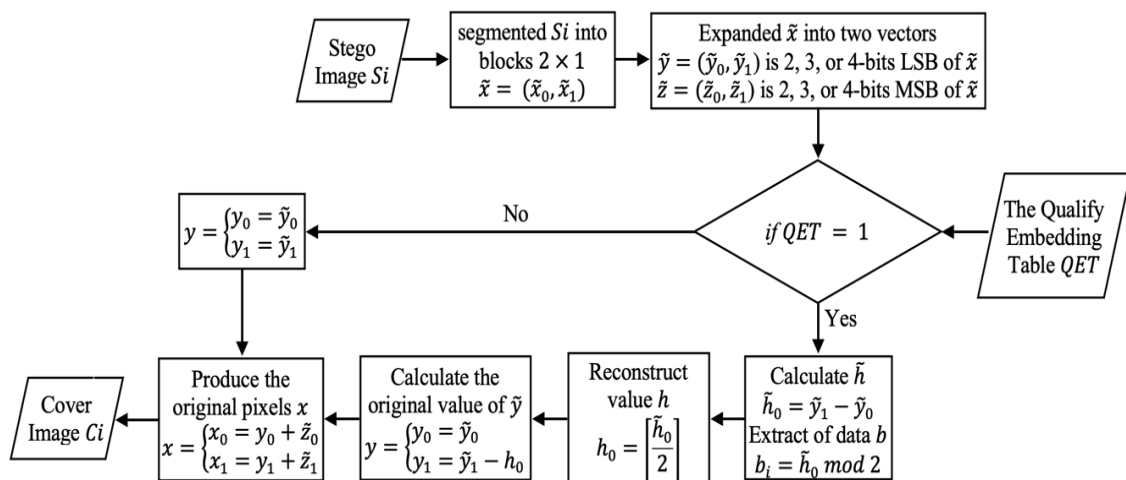


Figure 3. Extraction process for our method

2.1. Embedding procedure

The steps of the embedding process are similar to method [3], with the difference lying in the pre-embedding stage, where the pixel values of the image are divided into two components: the most significant bits (MSB) and the least significant bits (LSB). Subsequently, the LSB difference value of each pixel is utilized for data embedding. We propose three methods: first, using the difference in the 4-bit LSB values of pixel pairs; second, using the difference in the 3-bit LSB value of a pair of pixels; and third, using the difference in the 2-bit LSB value of a pair of pixels. This procedure of the embedding can be seen in Figure 2. The step-by-step embedding process is detailed as:

Step 1: Begin by dividing the cover image into 2×1 -sized blocks. Each pixel value within these blocks is then converted into 8-bits, producing a pixel vector representation labeled as $x = (x_0, x_1)$. These blocks are further expanded into two vectors: y , comprising the 4-bit, 3-bit, or 2-bit LSB of each x , and z , comprising the 4-bit, 5-bit, or 6-bit MSB of each x .

Step 2: Use (1) to calculate the difference value of pixel pairs in each block x and store them in the vector h .

$$h = y_1 - y_0 \quad (1)$$

Step 3: Examine the array h to identify values that satisfy the embedding criteria. Classify these values into two categories: if a value falls within the range of -2 to 2 ($-2 \leq h \leq 2$), mark it as qualified by setting $QET = 1$; otherwise, set $QET = 0$.

Step 4: Retrieve bit of the secret data in vector b . Apply (2) to embed the data, generating a new difference value represented as \tilde{h} . Each bit in b corresponds to a secret data bit, taking on a value of either 0 or 1.

$$\tilde{h} = h + b \quad (2)$$

Step 5: Use (3) to compute the new value of \tilde{y} as the sum of y_1 and h . (4) outline the conditions that must be met for our method in 4-LSB, 3-LSB, and 2-LSB pixels, respectively, to prevent overflow and underflow. If the conditions are met, the quality embedding table (QET) is set to 1; otherwise, if y falls outside the specified range, QET is set to 0, and y remains unchanged.

$$\tilde{y}_1 = y_1 + \tilde{h} \quad (3)$$

$$\tilde{y} = \begin{cases} 0 \leq y_1 + \tilde{h}_0 \leq 3. \text{ for } (2 - \text{bits}) \\ 0 \leq y_1 + \tilde{h}_0 \leq 7. \text{ for } (3 - \text{bits}) \\ 0 \leq y_1 + \tilde{h}_0 \leq 15. \text{ for } (4 - \text{bits}) \end{cases} \quad (4)$$

Step 6: Use (5) to reconstruct the new value of the block pixel \tilde{x} for the stego image by combining the \tilde{y} and z values.

$$\tilde{x} = \begin{cases} \tilde{x}_0 = \tilde{y}_0 + z_0 \\ \tilde{x}_1 = \tilde{y}_1 + z_1 \end{cases} \quad (5)$$

2.2. Extraction procedure

The extraction is similar to the embedding process, as illustrated in Figure 3. The steps for extraction are outlined:

Step 1: Begin by dividing the stego image into 2×1 -sized blocks. Each pixel value within these blocks is converted into 8-bits, resulting in a pixel vector representation denoted as $\tilde{x} = (\tilde{x}_0, \tilde{x}_1)$. These blocks are further expanded into two vectors: \tilde{y} , consisting of the 4-bit, 3-bit, or 2-bit LSB of each \tilde{x} , and \tilde{z} , consisting of the 4-bit, 5-bit, or 6-bit MSB of each \tilde{x} .

Step 2: Use (6) to calculate the difference value of pixel pairs in each block \tilde{x} and store them in the vector \tilde{h} .

$$\tilde{h} = \tilde{y}_1 - \tilde{y}_0 \quad (6)$$

Step 3: Extracting data from the difference value \tilde{h} involves utilizing the modulus function and the QET table, as outlined in (7)

$$b = \tilde{h} \bmod 2, \text{ if } QET = 1 \quad (7)$$

Step 4: Use (8) to reconstruct the original difference value of h from \tilde{h} , and use (9) to compute the original value of y from \tilde{y} . Afterward, use (10) to reconstruct the original pixel value of x by combining the y and \tilde{z} values.

$$h = \left\lceil \frac{\tilde{h}}{2} \right\rceil, \text{ if } QET = 1 \quad (8)$$

$$y = \begin{cases} y_0 = \tilde{y}_0 \\ y_1 = \tilde{y}_1 - h \end{cases} \quad (9)$$

$$x = \begin{cases} x_0 = y_0 + \tilde{z}_0 \\ x_1 = y_1 + \tilde{z}_1 \end{cases} \quad (10)$$

3. RESULTS AND DISCUSSION

To compare our proposed method with the method suggested by previous researchers in [3], we used six grayscale images. These included three common images (Baboon in Figure 4(a), Boat in Figure 4(b), and Lake in Figure 4(c)) and three medical images (Abdominal in Figure 4(d), Head in Figure 4(e), and CT scan in Figure 4(f)), obtained from the datasets provided in references [30], [31]. Each image had a resolution of 512×512 pixels. The experiments were conducted using MATLAB 2022b (license number 41125107) on an Intel Core i5 processor running at 2.9 GHz with 8 GB of memory.

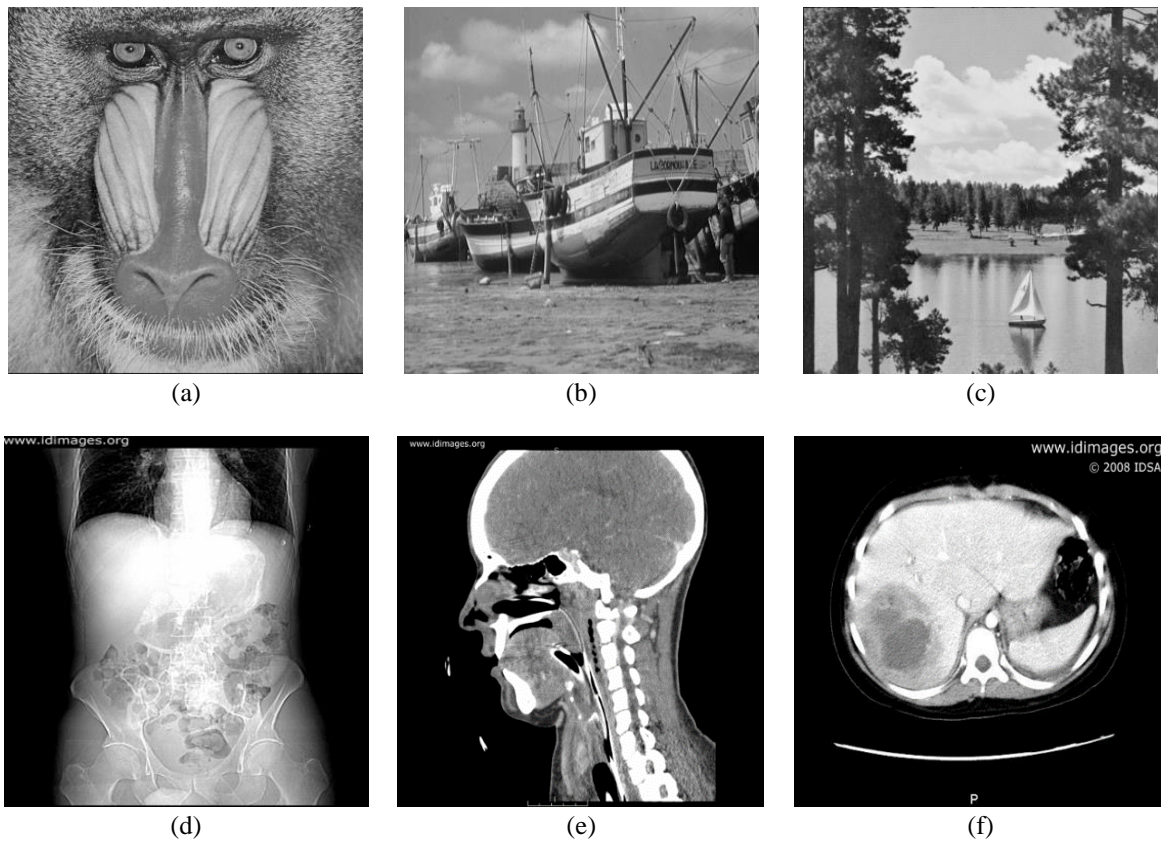


Figure 4. Sample images for testing; (a) Baboon, (b) Boat, (c) Lake, (d) Abdominal, (e) Head, and (f) CT scan

3.1. Embedding capacity

The results of the embedding capacity experiment are presented in Table 1 and Figure 5. Table 1 shows the capacity for embedding into the image that satisfies the embedding criteria for each method. The embedding capacity is the ratio of the total number of bits that can be embedded to the image resolution, measured in bits per pixel (bpp). Figure 5 illustrates how the embedding capacity varies across different

methods. Specifically, Figure 5(a) shows the maximum number of smooth pair images, and Figure 5(b) displays the embedding capacity (in bpp) for the images.

Table 1. Embedding capacity comparison

| | The embedding capacity in (bits) | | | | Embedding capacity (bpp) | | | |
|-----------|----------------------------------|-----------------|-----------------|-----------------|--------------------------|-----------------|-----------------|-----------------|
| | Maniriho and Ahmad [3] | Proposed 4-bits | Proposed 3-bits | Proposed 2-bits | Maniriho and Ahmad [3] | Proposed 4-bits | Proposed 3-bits | Proposed 2-bits |
| Baboon | 20,661 | 35,691 | 56,161 | 65,708 | 0.0788 | 0.1362 | 0.2142 | 0.2507 |
| Boat | 34,351 | 39,468 | 56,809 | 64,027 | 0.1310 | 0.1506 | 0.2167 | 0.2442 |
| Lake | 35,952 | 41,038 | 57,628 | 65,393 | 0.1372 | 0.1566 | 0.2198 | 0.2495 |
| Abdominal | 73,262 | 74,522 | 83,703 | 89,193 | 0.2795 | 0.2843 | 0.3193 | 0.3402 |
| Head | 84,306 | 88,193 | 96,784 | 100,902 | 0.3216 | 0.3364 | 0.3692 | 0.3849 |
| CT scan | 85,870 | 89,425 | 97,268 | 99,831 | 0.3276 | 0.3411 | 0.3711 | 0.3808 |

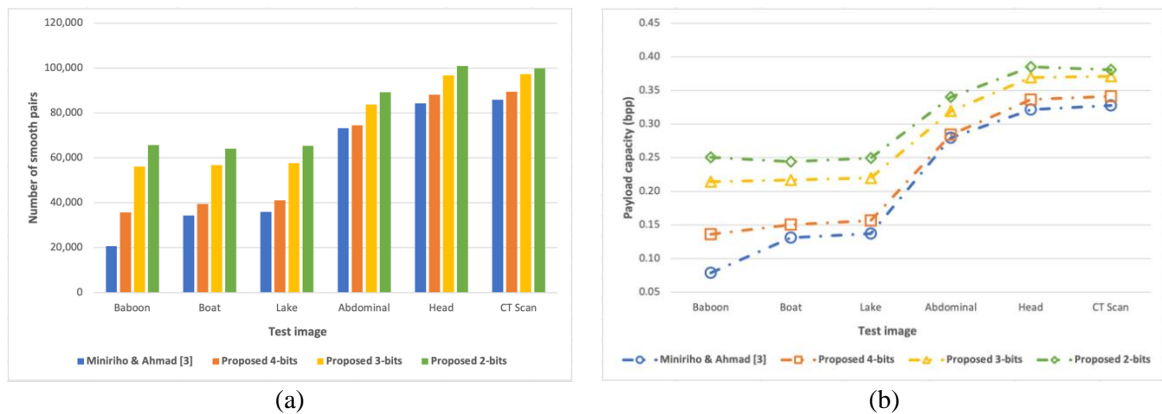


Figure 5. A comparison of our method with the previous approach in terms of; (a) the total number of smooth pair images and (b) embedding capacity (in bpp)

The experimental results show that our three proposed methods consistently achieve higher embedding capacities than method [3], as illustrated in Table 1 and Figure 5(a). This affirms that leveraging the difference values of the LSB in each pixel can enhance the number of pixel pairs meeting the embedding requirements. For instance, in a common image like Baboon, the embedding capacity of method [3] is 0.0788 bpp, whereas our proposed method, utilizing the difference value of the 4-bits LSB in each pixel, achieves a embedding capacity of 0.1362 bpp; for 3-LSB bits, it is 0.2142 bpp, and for 2-LSB bits, it is 0.2507 bpp. Similarly, in medical images like Abdominal, the embedding capacity of method [3] is 0.2795 bpp, while our proposed method, employing the difference value of the 4-bits LSB for each pixel, attains a embedding capacity of 0.2843 bpp; for 3-bits LSB, it is 0.3193 bpp, and for 2-bits LSB, it is 0.3402 bpp. Additionally, the experimental results reveal that the embedding capacities of method [3] and three of our proposed methods depend on the nature of the image. The embedding capacity tends to be higher in images with more smooth areas compared to those with fewer smooth areas, as illustrated in Figure 5(b). This can be observed in Table 1 and Figure 5, where the load capacity of medical images is significantly greater than that of general images. Based on the experiments that have been carried out, of three our proposed methods, utilizing the 2-bit LSB difference value has the highest embedding capacity.

3.2. Performance

The experimental results demonstrate that our proposed method excels in accurately extracting data and restoring the stego image to its original form, while preserving its visual quality. Regarding computational efficiency, our method outperforms method [3] across all experiments, as shown in Table 2. For the Baboon image, method [3] is capable of embedding only 4,666 bits of data per second. In contrast, our proposed method, utilizing the 4-bit LSB difference value, can embed 8,486 bits of data per second, and for the 3-bit LSB, it achieves 13,125 bits per second, while for the 2-bit LSB, it embeds 15,238 bits per second. Similarly, in medical images such as Abdominal images, method [3] can embed only 20,562 bits of data per second. On the other hand, our proposed method, using the 4-bit LSB difference value, achieves 20,805 bits per second, and for the 3-bit LSB, it embeds 23,387 bits per second, while for the 2-bit LSB, it

embeds 24,463 bits per second. Among three our proposed methods, using the 2-bit LSB difference value results in the fastest computational time.

Table 2. Comparison of computational time

| | Computational time (second) | | | | Embedding data in 1 seconds (bits) | | | |
|-----------|-----------------------------|-----------------|-----------------|-----------------|------------------------------------|-----------------|-----------------|-----------------|
| | Maniriho and Ahmad [3] | Proposed 4-bits | Proposed 3-bits | Proposed 2-bits | Maniriho and Ahmad [3] | Proposed 4-bits | Proposed 3-bits | Proposed 2-bits |
| Baboon | 4.43 | 4.21 | 4.28 | 4.31 | 4,666 | 8,486 | 13,125 | 15,238 |
| Boat | 3.59 | 3.62 | 3.60 | 3.61 | 9,561 | 10,918 | 15,780 | 17,746 |
| Lake | 3.77 | 3.79 | 3.76 | 4.14 | 9,546 | 10,819 | 15,318 | 15,815 |
| Abdominal | 3.56 | 3.58 | 3.58 | 3.65 | 20,562 | 20,805 | 23,387 | 24,463 |
| Head | 3.59 | 3.58 | 3.57 | 3.60 | 23,516 | 24,669 | 27,141 | 28,044 |
| CT scan | 3.85 | 3.59 | 3.58 | 3.90 | 22,315 | 24,903 | 27,177 | 25,631 |

3.3. Visual quality

Visual quality analysis was conducted to ensure that embedding data in the cover image did not significantly reduce its visual quality, causing distortion. The evaluation aimed to comprehend the impact of embedding capacity on the visual quality of the stego image, focusing on assessing fidelity and perception. Generally, as the embedded data increases, the visual quality of the stego image decreases. In this research, the peak signal-to-noise ratio (PSNR) is utilized to measure and compare the quality of the cover image and stego image using (11). The evaluation is performed with various data sizes ranging from 1 kb to 105 kb, with 5 kb intervals based on each method's capabilities.

$$PSNR = 10 \log_{10} \frac{255^2}{\frac{1}{m \times n} \sum_i^{m-1} \sum_j^{n-1} |I(i,j) - I'(i,j)|^2} \quad (11)$$

Table 3 provides a detailed PSNR measurement for embedding data with the maximum embedding in the test image for each method. Figure 6 compares the PSNR performance of our method with the previous method [3] across different embedding data sizes in each test image: Baboon (Figure 6(a)), Boat (Figure 6(b)), Lake (Figure 6(c)), Abdominal (Figure 6(d)), Head (Figure 6(e)), and CT scan (Figure 6(f)). The visual quality of the stego image with our proposed method is notably high. In various experiments, our proposed method exhibits a lower PSNR value compared to method [3], notably in 4-bit and 3-bit our methods. This is due to the larger volume of data embedded in our proposed method compared to method [3]. For a more accurate comparison, visual quality is presented in Figure 6, where the test compares equivalent data embedding sizes. The results consistently show that our proposed method achieves higher visual quality compared to the method in reference [3]. For example, in Baboon image with 20 kb of embedded data, the method in reference [3] achieves a PSNR value of 55.3858 dB, while our proposed method outperforms with values of 55.8161 dB in the 4-bit method, 56.5974 dB in the 3-bit method, and 60.5744 dB in the 2-bit method, as illustrated in Figure 6(a). Similarly, in Abdominal image with 60 kb of embedded confidential data, the method in [3] achieves a PSNR value of 54.0969 dB, whereas our proposed method demonstrates higher values, with 54.2734 dB in the 4-bit method, 54.3657 dB in the 3-bit method, and 56.6550 dB in the 2-bit method, as illustrated in Figure 6(d). Based on these results, our proposed method consistently delivers higher visual quality. Among the three proposed methods, the use of 2-bit LSB difference values achieves a significant increase in PSNR values compared to the method in reference [3].

Table 3. Comparing the quality of stego image using PSNR

| | Embedding capacity (bpp) | | | | PSNR (dB) | | | |
|-----------|--------------------------|-----------------|-----------------|-----------------|------------------------|-----------------|-----------------|-----------------|
| | Maniriho and Ahmad [3] | Proposed 4-bits | Proposed 3-bits | Proposed 2-bits | Maniriho and Ahmad [3] | Proposed 4-bits | Proposed 3-bits | Proposed 2-bits |
| Baboon | 0.0788 | 0.1362 | 0.2142 | 0.2507 | 55.2637 | 53.3199 | 52.1074 | 55.4145 |
| Boat | 0.1310 | 0.1506 | 0.2167 | 0.2442 | 53.1846 | 53.0564 | 52.2202 | 55.5230 |
| Lake | 0.1372 | 0.1566 | 0.2198 | 0.2495 | 52.9833 | 52.8596 | 52.0315 | 55.4190 |
| Abdominal | 0.2795 | 0.2843 | 0.3193 | 0.3402 | 52.9395 | 53.0756 | 52.6446 | 54.8443 |
| Head | 0.3216 | 0.3364 | 0.3692 | 0.3849 | 54.1959 | 53.8259 | 53.2164 | 54.6810 |
| CT scan | 0.3276 | 0.3411 | 0.3711 | 0.3808 | 53.7179 | 53.3644 | 52.8870 | 54.6022 |

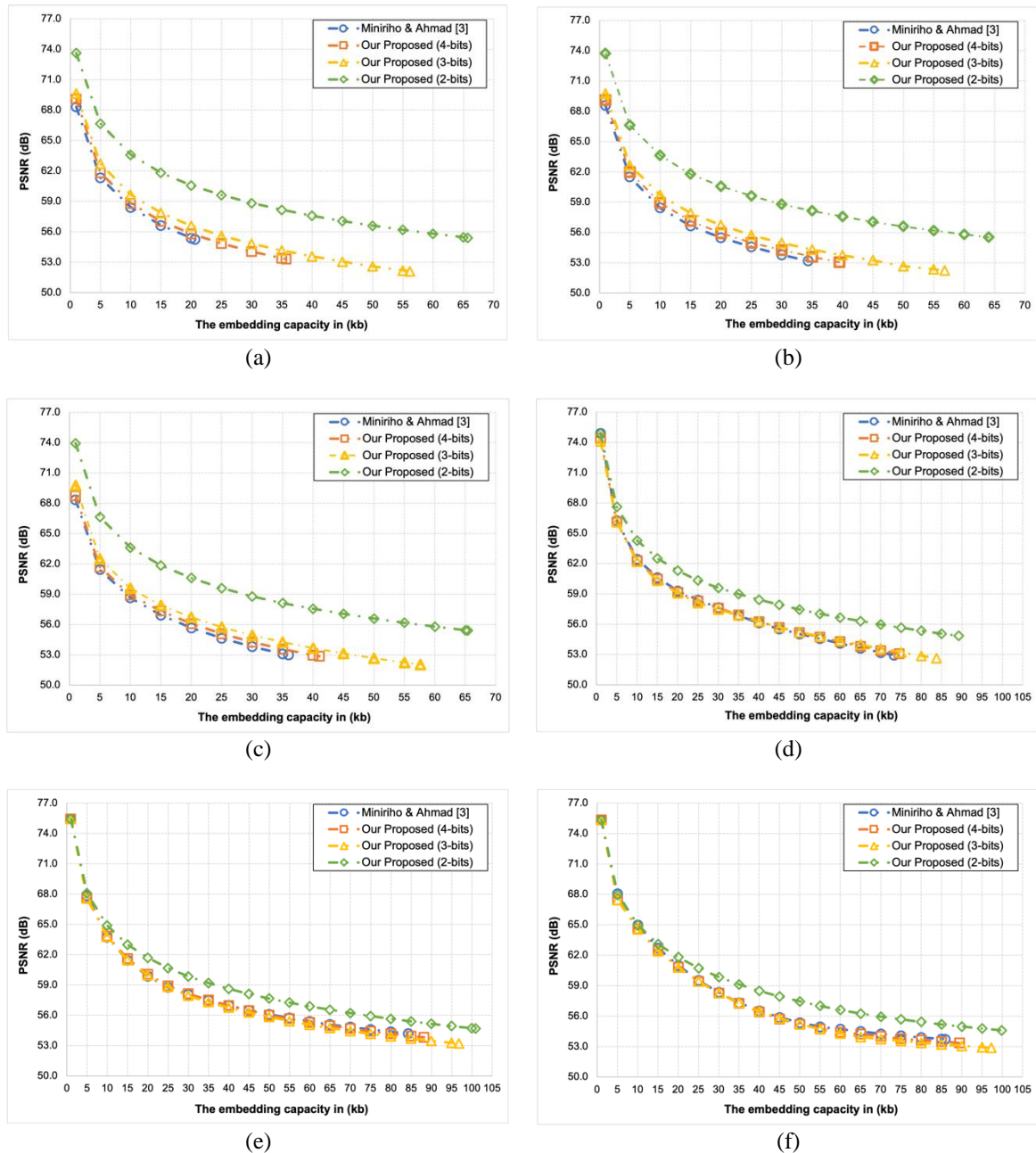


Figure 6. A comparison of our method with the previous method [3] in terms of PSNR across various embedding data sizes for the following images; (a) Baboon, (b) Boat, (c) Lake, (d) Abdominal, (e) Head, and (f) CT scan

4. CONCLUSION

The IoT provides numerous benefits to everyday life; however, its interconnected design introduces considerable challenges related to privacy and data security. Two primary techniques for addressing these issues are cryptography and steganography. Information security can be achieved through cryptography, which encrypts data to make it unreadable, or steganography, which hides data within other media. For sensitive media, such as military, medical, and forensic imaging, specialized techniques like RDH are necessary to ensure the media can be fully restored after data extraction. The DE method is widely recognized as an effective RDH technique because it allows the media to be restored to its original state after the secret data is extracted. In this research, we present an improved version of an RDH technique, which uses the difference values of the 4-bit, 3-bit, and 2-bit LSB of pixels. Our method embeds data within the difference values ranging from -2 to 2. Experiments conducted on three common images and three types of

medical images show that our approach achieves a high embedding capacity while maintaining excellent visual quality. The results indicate that our method outperforms existing techniques in terms of embedding capacity, performance, and visual fidelity. Furthermore, it provides strong security as a fragile data hiding approach, ensuring high-quality stego images even with substantial data embedding, thereby reducing the chances of detection by adversaries. To further enhance this method, future work should explore the potential of pixel difference values to increase both the embedding capacity and image quality. Additionally, encrypting sensitive data before embedding could be a promising direction for strengthening security in future research.

ACKNOWLEDGMENTS

The authors sincerely thank the Research and Community Service Institution (LPPM) of UIN Imam Bonjol Padang for their support in publishing this article, through the Litapdimas Research Grant 2024.

FUNDING INFORMATION

This research was funded by the Institute for Research and Community Service (LPPM), State Islamic University (UIN) Imam Bonjol Padang, under Grant Number 625/2024.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

| Name of Author | C | M | So | Va | Fo | I | R | D | O | E | Vi | Su | P | Fu |
|--------------------|---|---|----|----|----|---|---|---|---|---|----|----|---|----|
| Aulia Arham | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | | ✓ | ✓ | ✓ | | | ✓ | |
| Hanung Adi Nugroho | | ✓ | | | | ✓ | | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Domi Sepri | ✓ | | ✓ | ✓ | | | ✓ | | | ✓ | ✓ | | ✓ | ✓ |

| | | |
|-----------------------|--------------------------------|----------------------------|
| C : Conceptualization | I : Investigation | Vi : Visualization |
| M : Methodology | R : Resources | Su : Supervision |
| So : Software | D : Data Curation | P : Project administration |
| Va : Validation | O : Writing - Original Draft | Fu : Funding acquisition |
| Fo : Formal analysis | E : Writing - Review & Editing | |

CONFLICT OF INTEREST STATEMENT

The authors declare that they have no conflict of interest.

INFORMED CONSENT

This study did not involve human participants, personal data, or identifiable information; therefore, informed consent was not applicable.

ETHICAL APPROVAL

This study did not involve human participants or animals; therefore, ethical approval was not required.

DATA AVAILABILITY

<https://github.com/4rh4m/Reversible-data-hiding-with-selective-bits-difference-expansion-and-modulus-function>




REFERENCES

[1] H. Allioui and Y. Mourdi, "Exploring the Full Potentials of IoT for Better Financial Growth and Stability: A Comprehensive Survey," *Sensors*, vol. 23, no. 19. 2023. doi: 10.3390/s23198015.




[2] C. C. Islamy, T. Ahmad, and R. M. Ijtihadie, "Reversible data hiding based on histogram and prediction error for sharing secret data," *Cybersecurity*, vol. 6, no. 1, p. 12, 2023, doi: 10.1186/s42400-023-00147-y.

- [3] P. Maniriho and T. Ahmad, "Information hiding scheme for digital images using difference expansion and modulus function," *Journal of King Saud University - Computer and Information Sciences*, vol. 31, no. 3, pp. 335–347, 2019, doi: 10.1016/j.jksuci.2018.01.011.
- [4] H. A. Ali, A. J. Jalil, and M. K. Hussein, "Least significant bit technology for hiding text data using video steganography," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 22, no. 1, pp. 157–163, 2024, doi: 10.12928/TELKOMNIKA.v22i1.24029.
- [5] J. E. Nalavade, A. Patil, A. Buchade, and N. Jadhav, "Deep Neural Network and GAN-Based Reversible Data Hiding in Encrypted Images: A Privacy-Preserving Approach," *SN Computer Science*, vol. 5, no. 1, p. 45, 2024, doi: 10.1007/s42979-023-02347-2.
- [6] A. Arham and H. A. Nugroho, "Enhanced reversible data hiding using difference expansion and modulus function with selective bit blocks in images," *Cybersecurity*, vol. 4, no. 2, pp. 100–110, 2024, doi: 10.1186/s42400-024-00251-7.
- [7] M. H. Dehkordi *et al.*, "OTPT: A new steganography scheme with high capacity and security," *Multimedia Tools and Applications*, vol. 83, no. 6, pp. 17579–17599, 2024, doi: 10.1007/s11042-023-16312-x.
- [8] A. El Azzaoui, H. Chen, S. H. Kim, Y. Pan, and J. H. Park, "Blockchain-Based Distributed Information Hiding Framework for Data Privacy Preserving in Medical Supply Chain Systems," *Sensors*, vol. 22, no. 4, 2022, doi: 10.3390/s22041371.
- [9] H. T. Mangi, S. A. Ali, and M. J. Jawad, "Enhancing of coverless image steganography capacity based on image block features," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 21, no. 6, pp. 1364–1372, 2023, doi: 10.12928/TELKOMNIKA.v21i6.24816.
- [10] R. Anushkadevi and R. Amirtharajan, "Separable reversible data hiding in an encrypted image using the adjacency pixel difference histogram," *Journal of Information Security and Applications*, vol. 72, 2023, doi: 10.1016/j.jisa.2022.103407.
- [11] S. Gull, N. A. Loan, S. A. Parah, J. A. Sheikh, and G. M. Bhat, "An efficient watermarking technique for tamper detection and localization of medical images," *Journal of Ambient Intelligence and Humanized Computing*, vol. 11, no. 5, pp. 1799–1808, May 2020, doi: 10.1007/s12652-018-1158-8.
- [12] S. Kanwal, F. Tao, A. Almogren, A. Ur Rehman, R. Taj, and A. Radwan, "A Robust Data Hiding Reversible Technique for Improving the Security in e-Health Care System," *CMES - Computer Modeling in Engineering and Sciences*, vol. 134, no. 1, pp. 201–219, 2023, doi: 10.32604/cmes.2022.020255.
- [13] K. Nour and A. Al-Haj, "Reversible data hiding using bit flipping and histogram shifting," *Multimedia Tools and Applications*, vol. 81, no. 9, pp. 12441–12458, 2022, doi: 10.1007/s11042-022-12364-7.
- [14] V. M. Devineni, V. N. D. Pavuluri, and V. M. Manikandan, "A Detailed Review on Reversible Data Hiding and Its Applications," in *Lecture Notes in Networks and Systems*, Springer, 2023, pp. 413–423, doi: 10.1007/978-3-031-27524-1_39.
- [15] J. Tian, "Reversible Data Embedding Using a Difference Expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890–896, 2003, doi: 10.1109/TCSVT.2003.815962.
- [16] Z. Syahlan and T. Ahmad, "Reversible data hiding method by extending reduced difference expansion," *International Journal of Advances in Intelligent Informatics*, vol. 5, no. 2, pp. 101–112, 2019, doi: 10.26555/ijain.v5i2.351.
- [17] M. S. Hossen, T. Ahmad, and N. J. D. La Croix, "Data Hiding Scheme using Difference Expansion and Modulus Function," in *2023 2nd International Conference for Innovation in Technology, INOCON 2023*, 2023, pp. 1–6, doi: 10.1109/INOCON57975.2023.10100991.
- [18] D. M. Thodi and J. J. Rodríguez, "Expansion embedding techniques for reversible watermarking," *IEEE Transactions on Image Processing*, vol. 16, no. 3, pp. 721–730, 2007, doi: 10.1109/TIP.2006.891046.
- [19] X. Wang, X. Wang, B. Ma, Q. Li, and Y. Q. Shi, "High Precision Error Prediction Algorithm Based on Ridge Regression Predictor for Reversible Data Hiding," *IEEE Signal Processing Letters*, vol. 28, pp. 1125–1129, 2021, doi: 10.1109/LSP.2021.3080181.
- [20] R. Hu and S. Xiang, "CNN prediction based reversible data hiding," *IEEE Signal Processing Letters*, vol. 28, pp. 464–468, 2021, doi: 10.1109/LSP.2021.3059202.
- [21] L. Li, Y. Yao, and N. Yu, "High-fidelity video reversible data hiding using joint spatial and temporal prediction," *Signal Processing*, vol. 208, 2023, doi: 10.1016/j.sigpro.2023.108970.
- [22] N. Mao, F. Chen, H. He, and Y. Yang, "Reversible data hiding based on adaptive IPVO and two-segment pairwise PEE," *Signal Processing*, vol. 198, 2022, doi: 10.1016/j.sigpro.2022.108577.
- [23] N. Kumar, R. Kumar, A. Malik, S. Singh, and K. H. Jung, "Reversible data hiding with high visual quality using pairwise PVO and PEE," *Multimedia Tools and Applications*, vol. 82, no. 20, pp. 30733–30758, 2023, doi: 10.1007/s11042-023-14867-3.
- [24] Z. Ni, Y. Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354–361, 2006, doi: 10.1109/TCSVT.2006.869964.
- [25] A. Sukumar, V. Subramaniaswamy, L. Ravi, V. Vijayakumar, and V. Indragandhi, "Robust image steganography approach based on RIWT-Laplacian pyramid and histogram shifting using deep learning," *Multimedia Systems*, vol. 27, no. 4, pp. 651–666, 2021, doi: 10.1007/s00530-020-00665-6.
- [26] B. He, Y. Chen, Y. Zhou, Y. Wang, and Y. Chen, "A novel two-dimensional reversible data hiding scheme based on high-efficiency histogram shifting for JPEG images," *International Journal of Distributed Sensor Networks*, vol. 18, no. 3, 2022, doi: 10.1177/15501329221084226.
- [27] O. S. Faragallah, M. A. Elaskily, A. F. Alenezi, H. S. El-sayed, and H. M. Kelash, "Quadruple histogram shifting-based reversible information hiding approach for digital images," *Multimedia Tools and Applications*, vol. 80, no. 17, pp. 26297–26317, 2021, doi: 10.1007/s11042-021-10956-3.
- [28] L. Tanwar and J. Panda, "Hybrid reversible watermarking algorithm using histogram shifting and pairwise prediction error expansion," *Multimedia Tools and Applications*, vol. 83, no. 8, pp. 22075–22097, 2024, doi: 10.1007/s11042-023-15508-5.
- [29] F. Ren, Y. Liu, X. Zhang, and Q. Li, "Reversible information hiding scheme based on interpolation and histogram shift for medical images," *Multimedia Tools and Applications*, vol. 82, no. 18, pp. 28445–28471, 2023, doi: 10.1007/s11042-022-14300-1.
- [30] "USC-SIPI," SIPI Image Database. [Online]. Available: <https://sipi.usc.edu/database/database.php?volume=misc> (Accessed: Jan. 09, 2024).
- [31] "Partners Infectious Disease Images, Emicrobes Digital Library," www.idimages.org. [Online]. Available: <http://www.idimages.org/images/browse/ImageTechnique/> (Accessed: May 05, 2024).




BIOGRAPHIES OF AUTHORS

Aulia Arham    received the B.Sc. degree in Informatics Engineering from the Sekolah Tinggi Manajemen Informatika dan Komputer Duta Bangsa (STMIKDB), Surakarta, Indonesia and the M.S. degree in Electrical Engineering at Universitas Gadjah Mada, Yogyakarta, Indonesia, in 2016. Since 2018, he is appointed as lecturer in the Department of Information System, Faculty of Science and Tehnology, Universitas Islam Negeri Imam Bonjol, Padang, Indonesia. His research interests are watermarking, steganography, cryptography, security, image processing, and medical imaging. He can be contacted at email: auliaarham@uinib.ac.id.



Hanung Adi Nugroho    received the B.Eng. degree in electrical engineering from Universitas Gadjah Mada, Indonesia, 2001 and Master of Engineering degree in Biomedical Engineering from the University of Queensland, Australia in 2005. In 2012, he received his Ph.D. deegree in Electrical and Electronic Engineering from Universiti teknologi Petronas, Malaysia. Currently, he is a Professor and also a Head of Department of Electrical and Information Engineering, Faculty of Engineering, Universitas Gadjah, Yogyakarta, Indonesia. His current research interests include biomedical signal and image processing and analysis, computer vision, medical instrumentation, and pattern recognition. He can be contacted at email: adinugroho@ugm.ac.id.



Domi Sepri    received the B.Eng. degrees in Informatics Engineering from Universitas Islam Negeri Sultan Syarif kasim, Pekanbaru, Indonesia, in 2014 and M.S degree in Universitas Putra Indonesia YPTK Padang in 2016. He has been designated as a lecturer within the Department of Information Systems at the Faculty of Science and Technology, Universitas Islam Negeri Imam Bonjol, located in Padang, Indonesia. His research interests are analysis information system and data science. He can be contacted at email: domisepri@uinib.ac.id.